Information Technology (IT) Security Audit Standard

Issue Date: June 1, 2004
Effective Date: June 1, 2004

Number: HHSS-2004-002-A

1.0 Purpose

This standard defines guidelines used to perform Information Technology (IT) Security Audit(s) on HHSS IT systems, hardware, or business processes using IT resources. IT Security Audits of HHSS IT resources are conducted to:

- Ensure integrity, confidentiality and availability of information and resources.
- Investigate possible security incidents and ensure conformance to HHSS security polices and standards.
- Monitor user or system activity where appropriate.
- Initiate an appropriate remediation plan for policy violations or security vulnerabilities identified.

2.0 Scope

This standard applies to employees, contractors, consultants, temporary employees, volunteers, and other workers employed by HHSS.

IT Security Audits may be conducted on:

- Software applications (commercial and internally developed) owned or supported by HHSS.
- All HHSS and State IT resources owned or supported by HHSS including, servers, workstations, PDAs, wireless devices, routers, switches, hubs, laptop computers, and home computers used exclusively for HHSS work activity.
- Network, LAN, or application access.
- Business processes employing IT resources.
- Outside entities that have signed a *Third Party Agreement* with HHSS.

3.0 Standard

This standard provides guidelines for compliance to the Information Technology Security Policy No. HHS-2004-002.

The HHSS IT Security Administrator or designated team using the guidelines defined in this document will conduct IT Security Audits of HHSS IT resources with the express purpose of:

- Ensure integrity, confidentiality, and availability of information and IT resources.
- Investigate security incidents and conformance to HHSS IT Policies.
- Monitor user or system activity when and where appropriate.
- Develop and implement remediation plans.

It is the responsibility of the HHSS Entity responsible for an IT resource to maintain internal audit tools and or logs sufficient to provide proof of compliance with HHSS IT Policies and Nebraska and Federal regulations. Employees will cooperate fully with any IT audit conducted on systems for which they are held accountable.

Development and implementation of remediation programs as a result of an IT Security Audit is the joint responsibility of the HHSS Entity responsible for the IT resource audited, IS&T, and IT Security Administrator.

3.1 IT Security Audit Schedule.

3.1.1 Scheduled and periodic IT audits will be conducted on HHSS IT resources as a joint venture between IS&T, the HHSS entity being audited, and IT Security Administrator.

3.1.2 LAN Access logs must be reviewed by LAN Administration on a weekly basis in accordance with the Audit Review Procedures associated with this standard.

3.1.3 Application Access logs (including RACF logs) must be reviewed by and assigned auditor (for each application) on a weekly basis in accordance with the Audit Review Procedure associated with this standard.

3.1.4 IT Security Administrator will review Access Log findings and procedures with Access Log monitors on a quarterly basis.

3.1.5 Audit procedures will be reviewed on an annual basis by a Security Review Team appointed by the IS&T Administrator or their appointed agent.

3.2 Audit Access

3.2.1 When requested for the purpose of performing an IT audit of an HHSS IT Resource, any and all access required will be provided to the IT Security Administrator or the assigned audit team.

3.2.1.1 This access may include:

- Access to all electronic access, system, and audit logs
- All active and inactive email accounts.
- Database logs.
- Access to hardware owned or supported by HHSS (i.e. workstations, servers, PDAs, communication equipment)
- Access to information (electronic, hardcopy, etc.) that may be produced transmitted or stored on HHSS equipment or premises.
- Access to work areas (labs, offices, cubicles, storage areas, etc.).
- Access to interactively monitor and log traffic on HHSS networks.

3.3 Audit Procedures

3.3.1 Each program area that owns, manages or is assigned IT resources to be audited will develop appropriate audit procedures and will designate staff to perform reasonable and appropriate audits.

3.3.2 IS&T will work in partnership with program areas to identify and develop reasonable and appropriate audit procedures that meet HHSS security safeguards and Nebraska and Federal regulatory requirements.

3.3.3 Review of audit findings and procedures will be conducted on a periodic basis to maintain a reasonable and appropriate level of safeguards. This review will be a joint effort between the IT Security Administrator, IS&T, and the HHSS entity responsible for the resource(s) being audited.

3.3.4 HHSS staff, contractors and contracted business partners are expected to cooperate fully when audit procedures or reviews are initiated.

3.3.5 Safeguard or policy violations or incidents should be reported as defined in IT policy standard HHSS 2004-002-C.

4.0 Enforcement

Should a violation of this IT Security Standard occur, the individual(s) who committed the violation will be personally liable for their actions or the actions taken by others due to their violation of this standard. Lack of knowledge of or familiarity with this policy shall not release an individual from such liability. Any employee found to have violated this standard may be subject to disciplinary action, as defined in the governing policy HHS 2004 -002

5.0 Revision History

HR Legal – 03/12/2004

CCT Approval – 05/27/2004